JWT SECURITY MISCONFIGURATION

Leslie Jones | 05Dec2025

Challenge: JWT SECURITY MISCONFIGURATION - HIGH SEVERITY

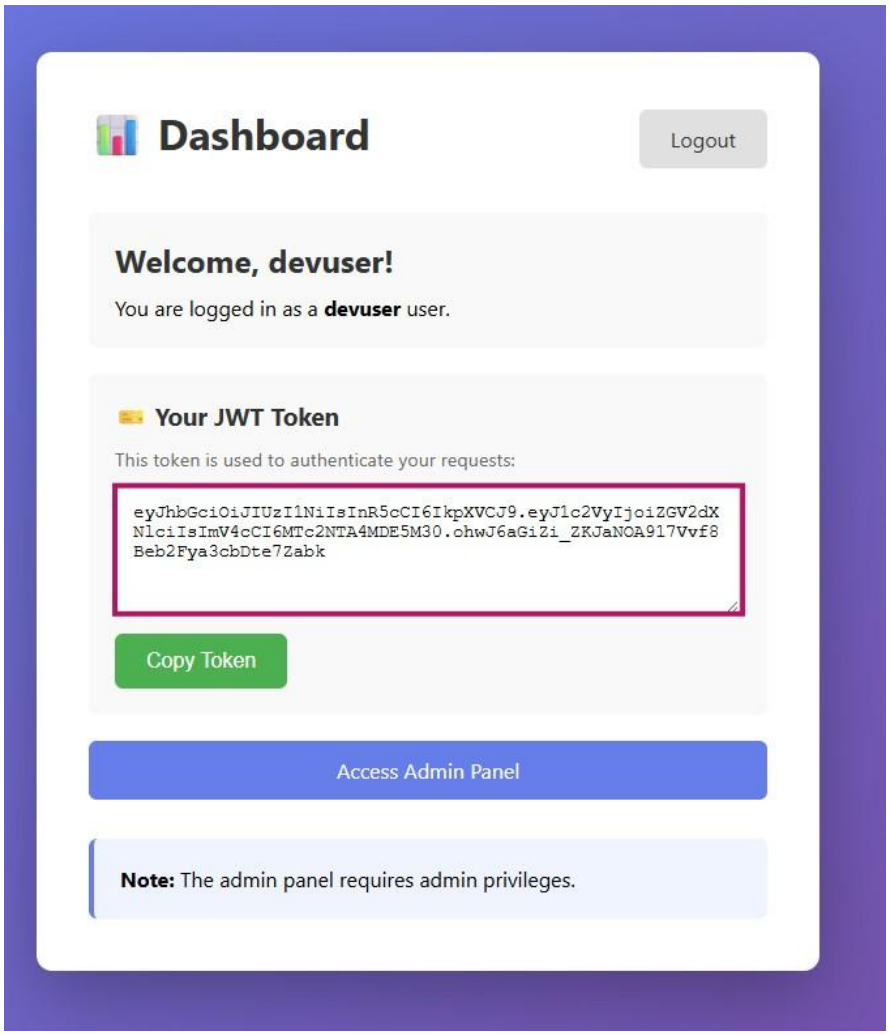
CWE-345: Insufficient Verification of Data Authenticity
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

SUMMARY

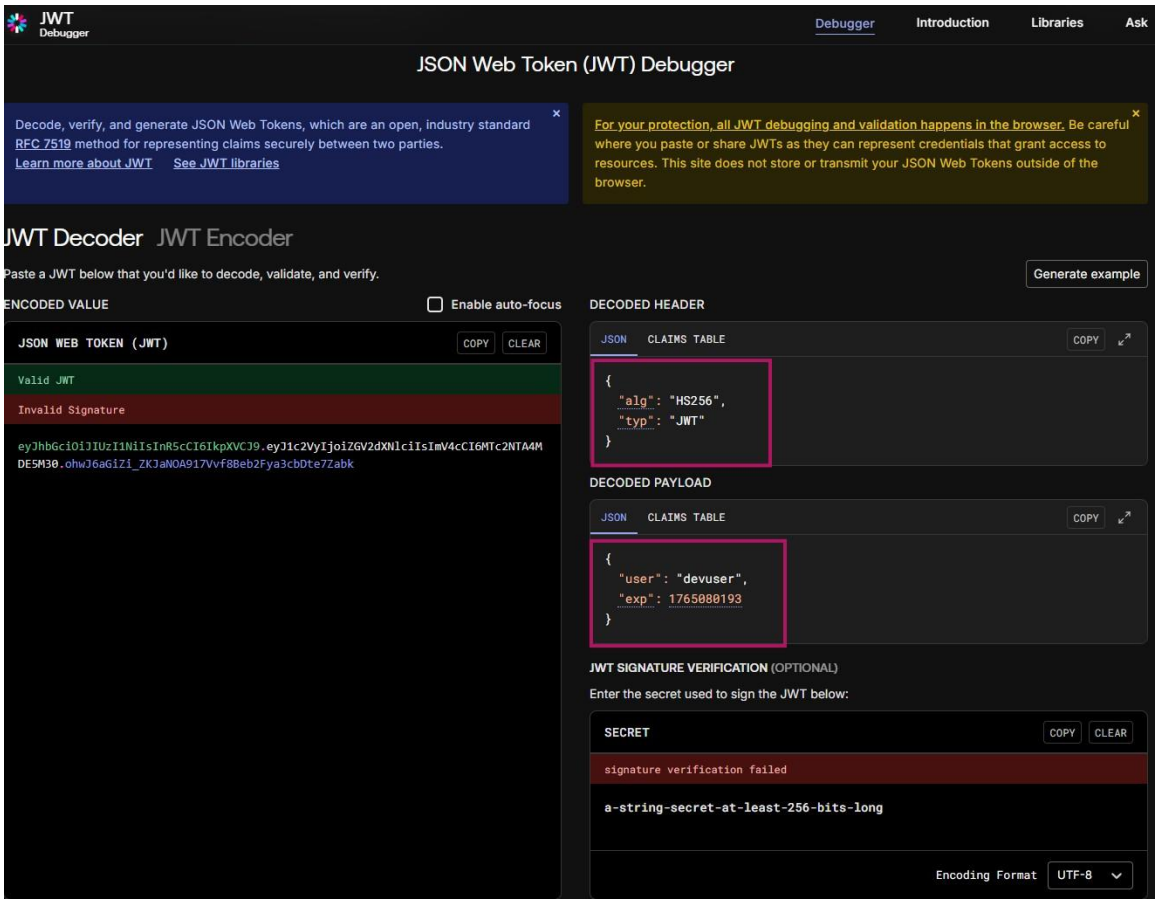
The web application that utilized JSON Web Tokens for authentication. Using HS256 as the signing algorithm, but setting a weak passphrase as the secret key. With the jwt_tool I was able to brute-force the signing key and modify the JWT payload to escalate privileges from devuser to admin.

STEPS TO REPRODUCE

1. Login to the environment to retrieve JWT token
   With the login credentials provided I logged into the environment and copied the token

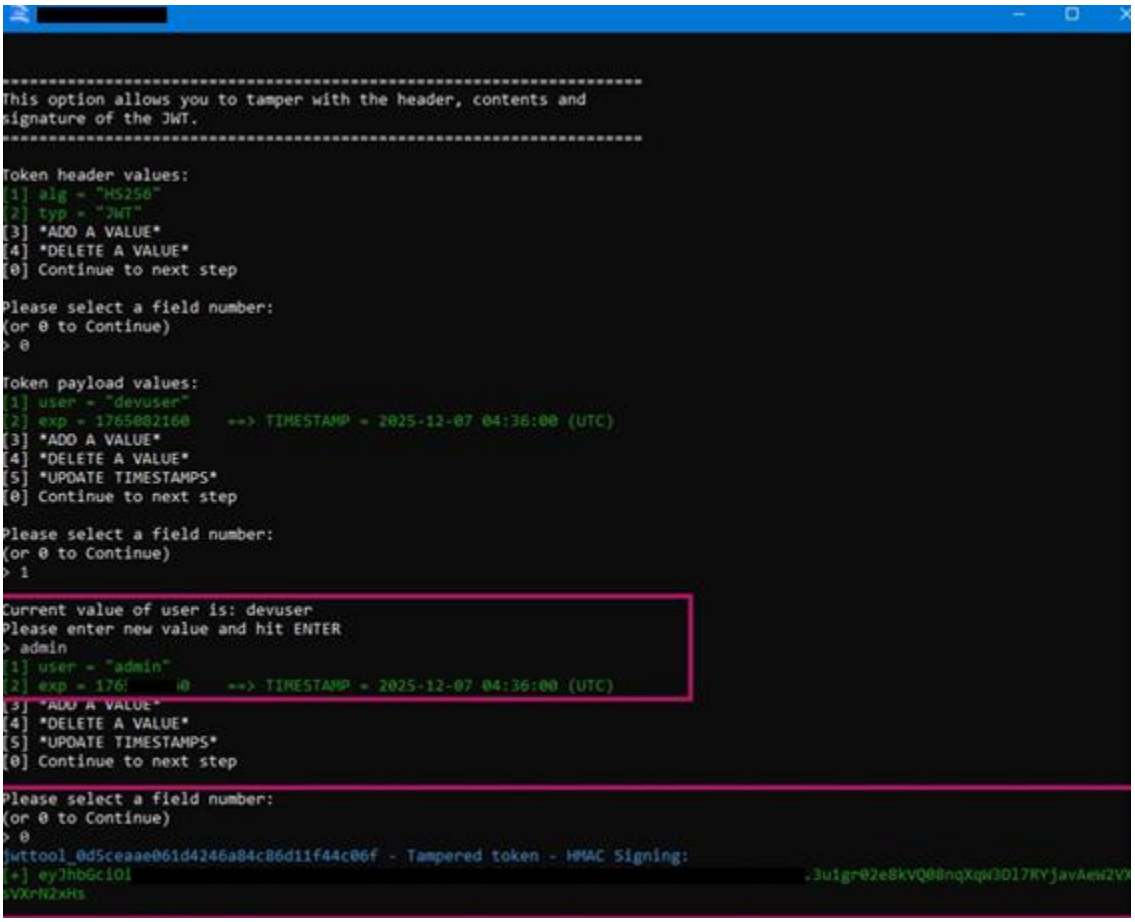


2. Decode the JWT token
   Transferring the token into https://www.jwt.io/ I was able to break down the header, payload, and secret key.

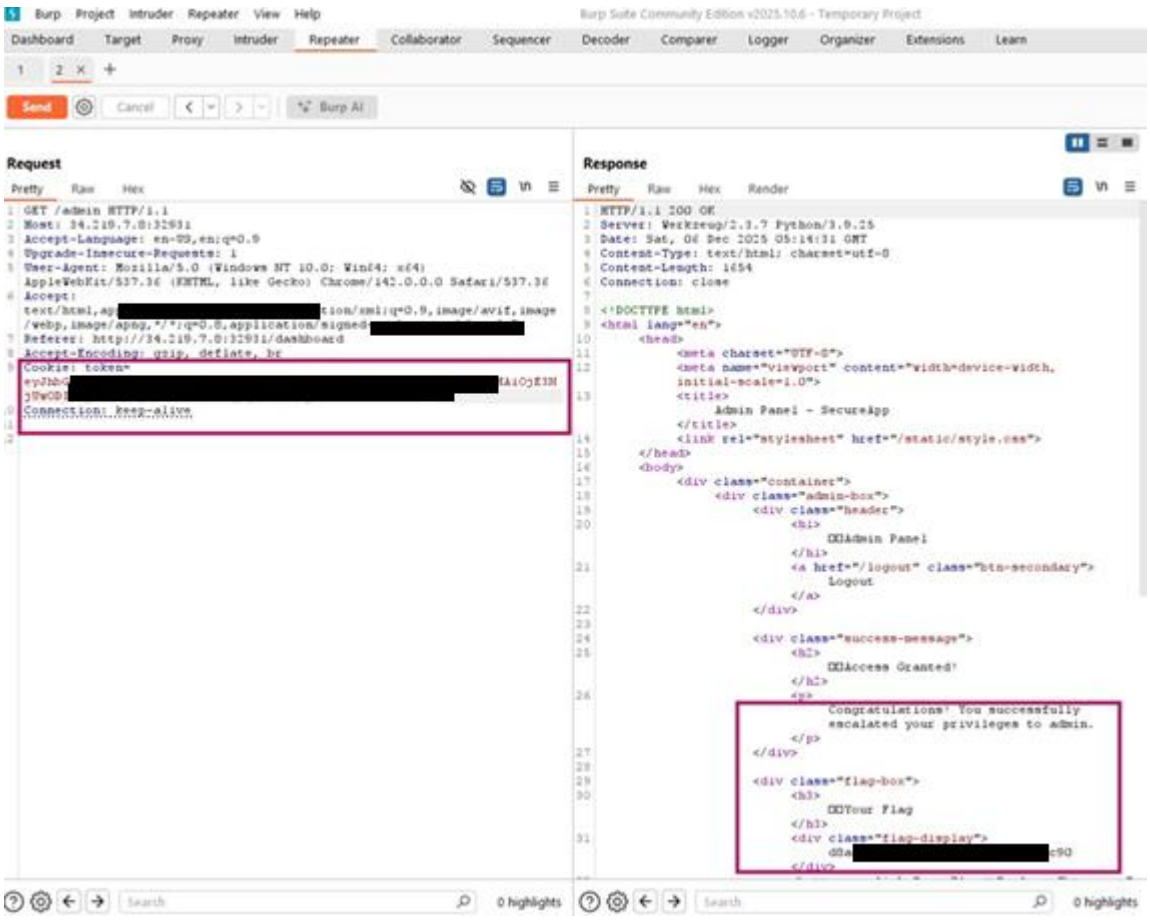


3. Brute force the secret key
   Within the terminal I ran the jwt_tool alongside a wordlist to decode the secret key

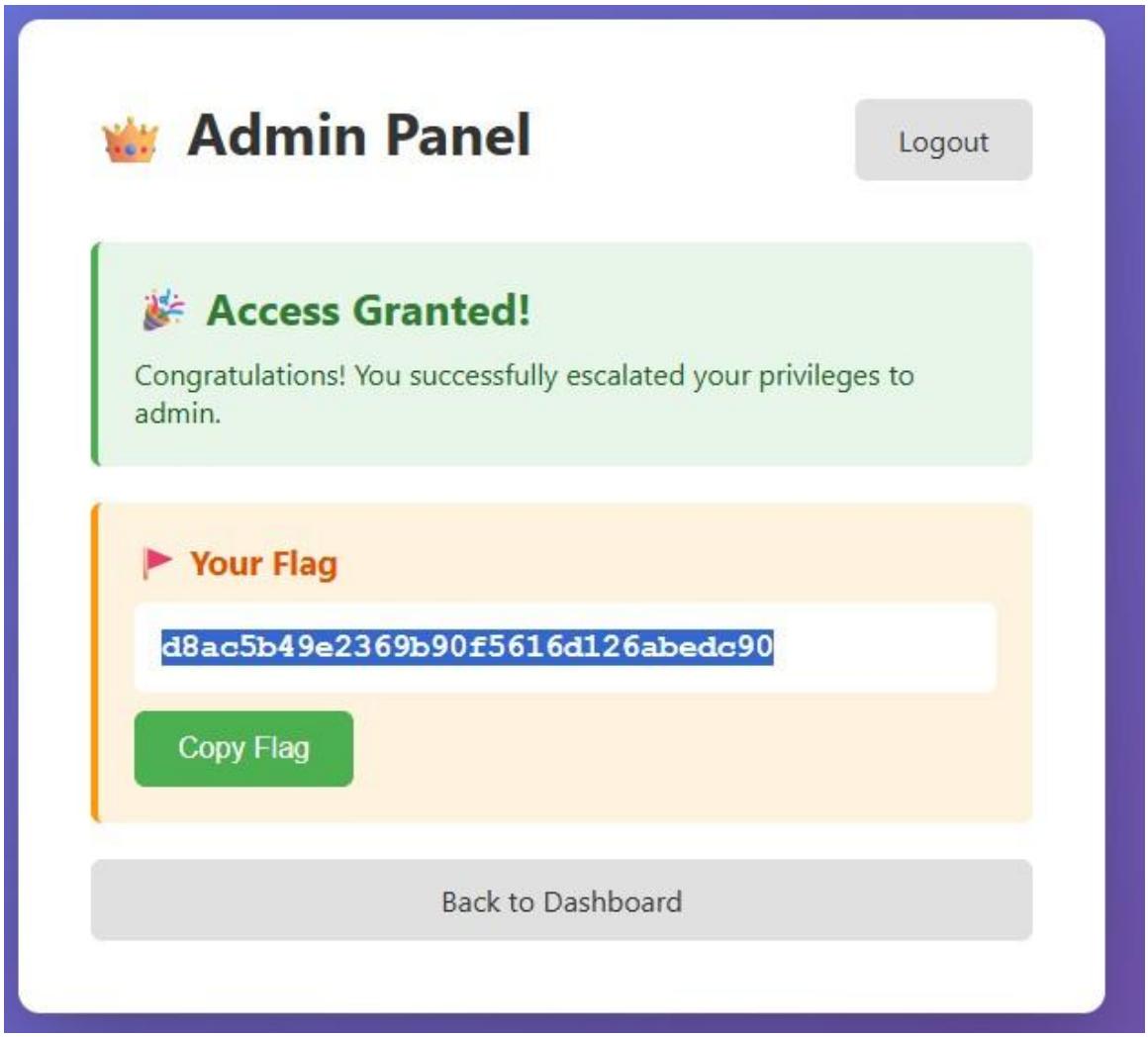
4. Alter the token for escalation
   Once the secret key was exposed, I modified the token with the user “admin” and ensured it was resigned with the key for continued access in the web environment



5. Test modified token with Burp Suite
   Before testing in the environment, I pasted the forged token in the Burp Suite Repeater environment to ensure the response would be “200 OK”



6. Update token and refresh page
   With confirmed response in Burp suite, I updated the JWT token and forwarded the packets, resulting in successful escalation as admin and flag retrieval



REMEDIATION STEPS

- Use strong key signing secrets to prevent attackers from easily cracking/altering the key
- Rotate JWT secrets regularly and invalidate tokens signed with old keys
- Set short expiration times and require re-authentication for privileged actions
- Monitor authentication logs for token abuse

REFERENCES

- CWE - CWE-345: Insufficient Verification of Data Authenticity (4.18)
- OWASP Top Ten 2004 Category A3 - Broken Authentication and Session Management | Martello Security

- JSON Web Tokens - jwt.io
- JWT attacks | Web Security Academy
- GitHub - ticarpi/jwt_tool: :snake: A toolkit for testing, tweaking and cracking JSON Web Tokens